UNITED STATES DISTRICT COURT

for the
District of Arizona

In the Matter of the Search of information associated with brianbown@hotmail.com that is stored at premises owned or controlled by Microsoft Corporation	Case No. 21-5244MB

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer:

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Western District of Washington:

As further described in Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal:

As set forth in Attachment B.

YOU ARE COMMANDED to execute this warrant on or before November 8, 2021 *(not to exceed 14 days)*
☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to any United States Magistrate Judge on criminal duty in the District of Arizona.

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized ☐ for 30 days (*not to exceed 30*) ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: Oct. 25, 2021 @ 11:36 a.m.

Judge's signature

City and state: Phoenix, Arizona

Honorable Deborah M. Fine, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with brianbown@hotmail.com that is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, a company headquartered at 1 Microsoft Way, Redmond, WA 98052.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Microsoft Corporation (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account from March 2, 2021, through the present, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence and instrumentalities of Interstate Communications Involving a Threat, in violation of 18 U.S.C. § 875(c), as well as Cyberstalking, in violation of 18 U.S.C. § 2261A(2) and 2261(b) (the "target offenses"), those violations involving Brian Bown and occurring after March 2, 2021, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Evidence of threats toward members of the Federal Public Defender's Office in the District of Arizona, including victim M.R.;

(b) Evidence of any investigations done on members of the Federal Public Defender's Office in the District of Arizona, including victim M.R., such as photographs of the victim, research or searches for the victim's residence, maps of the area near the attorney's residence, and other information that could be used to carry out a threat;

(c) Records, documents, communications, or other information indicating planning, intent, state of mind, or motive to commit the target offenses;

(d) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(e) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(f) The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s).

(g) The identity of any person(s) who communicated with the account about matters relating to the target offenses.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, investigating agents may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

AO 106 Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
District of Arizona

In the Matter of the Search of information associated with brianbown@hotmail.com that is stored at premises owned or controlled by Microsoft Corporation	Case No. 21-5244MB

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

As further described in Attachment A

located in the Western District of Washington, there is now concealed:

As set forth in Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code/Section	*Offense Description*
18 U.S.C. § 875(c)	Interstate Communications Involving a Threat
18 U.S.C. § 2261A(2) and 2261(b)	Cyberstalking

The application is based on these facts:

See Affidavit of Probable Cause, Incorporated by Reference

☒ Continued on the attached sheet.

☐ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA
William G. Voit

Digitally signed by WILLIAM VOIT
Date: 2021.10.25 08:40:11 -07'00'

Charles Rowland
Applicant's Signature

Charles Rowland, Senior Inspector, USMS
Printed name and title

Subscribed and sworn to telephonically:

Date Oct. 25, 2021 @ 11:36 a.m.

Judge's signature

City and state: Phoenix, Arizona

Honorable Deborah M. Fine, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with brianbown@hotmail.com that is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, a company headquartered at 1 Microsoft Way, Redmond, WA 98052.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Microsoft Corporation (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account from March 2, 2021, through the present, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence and instrumentalities of Interstate Communications Involving a Threat, in violation of 18 U.S.C. § 875(c), as well as Cyberstalking, in violation of 18 U.S.C. § 2261A(2) and 2261(b) (the "target offenses"), those violations involving Brian Bown and occurring after March 2, 2021, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Evidence of threats toward members of the Federal Public Defender's Office in the District of Arizona, including victim M.R.;

(b) Evidence of any investigations done on members of the Federal Public Defender's Office in the District of Arizona, including victim M.R., such as photographs of the victim, research or searches for the victim's residence, maps of the area near the attorney's residence, and other information that could be used to carry out a threat;

(c) Records, documents, communications, or other information indicating planning, intent, state of mind, or motive to commit the target offenses;

(d) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(e) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(f) The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s).

(g) The identity of any person(s) who communicated with the account about matters relating to the target offenses.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, investigating agents may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

AFFIDAVIT OF PROBABLE CAUSE

IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Charles Rowland, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account (brianbown@hotmail.com) that is stored at premises controlled by Microsoft Corporation ("Microsoft"), an email provider headquartered at 1 Microsoft Way, Redmond, WA 98052. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Microsoft Corporation to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Senior Inspector (SI) with the United States Marshals Service (USMS), and I have been so employed for approximately eighteen years. As an SI of the USMS, I am an investigative or law enforcement officer within the meaning of Section 2510(7) of Title 18 of the United States Code; that is, I am an officer of the United States who is authorized by law to conduct investigations of, and make arrests for, offenses enumerated in Title 18.

3. I am assigned to the Judicial Security Unit (JSU). In the course of my official duties, I am charged with the investigation of crimes involving the violation of offenses under Title 18, including cyberstalking and threatening interstate communications. The following information was developed by me and/or provided to me by other law enforcement officers, and other persons, in connection with the USMS investigation. The information contained in this affidavit is from my personal knowledge, as well as from information provided to your affiant by other law enforcement officers and/or witnesses,

including those listed herein. Due to the fact that this affidavit is being made to establish probable cause, your affiant has not listed each and every fact known regarding this investigation.

4. The facts of this case, briefly summarized, are that on or about and between October 20, 2021, and October 21, 2021, in the District of Arizona and elsewhere, there is probable cause to believe that Brian Gillespie Bown ("Bown") committed Interstate Communications Involving a Threat, in violation of 18 U.S.C. § 875(c), as well as Cyberstalking, in violation of 18 U.S.C. § 2261A(2) and 2261(b) (the "target offenses"), by sending emails to an attorney at the Federal Public Defender's Office in the District of Arizona, whose initials are "M.R." (hereinafter, "the victim"). Bown is believed to be a potential witness in a criminal case currently pending in this District.

5. In the emails, Bown appears to be demanding that he be provided with a recording made at his residence in the possession of the victim. He threatens that the attorney has one week to return the recording "[o]r you better start wearing a flak jacket," he tells the attorney "I know where you live," and he repeatedly uses vulgar, derogatory, and harassing epithets in the course of demanding that the recording be provided to him.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to search the information described in Attachment A for evidence and instrumentalities of these crimes further described in Attachment B.

JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

8. On or about October 20, 2021, your affiant was contacted by staff from the Federal Public Defender's Office (FPD) regarding threats received by a staff member. The FPD forwarded to the U.S. Marshals three emails, reproduced below, from email address

"brianbown@hotmail.com." The emails were directed to the victim at his work email address at the FPD, and at least one email also copied L.C. (whom I know to be an FPD investigator), also using his FPD email address.

9. The following are the contents of the three emails provided to me by the FPD:

a. On 10/20/2021 from brianbown@hotmail.com: "I have previously politely asked for a copy of the tape made at my house. This is my second request. You better fucking give me a copy you fucking, lying cunt. I am moving so you have 1 week you cunt. Or you better start wearing a flak jacket. You manipulated me, lied to me, and your client is going to be buried nbecause you are scum working for lesbian Eileen Willett. I I own my image, my voice likeness, and you have no right to use it. Return it or else. Fuck you." The initials bb were located at the end of the email content.

b. On 10/21/2021 from brianbown@hotmail.com: "Fucking give me a copy you cunt. I will be posting a sign at your office, and I know where you live cunt. I am not a violent person. Could harm no one. But I will write about a lying cunt lawyer til you go to your firm when yur done destroying lives. Where is that tape I want it bitch. BLOCK ME CUNT".

c. On 10/21/2021 from brianbown@hotmail.com: "Until you send me a copy of that tape you cunt I will do everything to get itbyoubfucking, vscumbag lying bitch. You better fucking comply cunt. Maybe you can get lesbian Eileen Wilkett to help you".

10. The user of the "brianbown@hotmail.com" email account is believed to be Brian Bown, then residing at a mobile home complex in Phoenix, Arizona. I understand that Bown was a potential witness in the case of *United States v. Jerry Wayne Story, II*, No. CR 21-00206-PHX-DJH (D. Ariz.). In that case, Story was charged for making threats against a person protected by the U.S. Secret Service. Victim M.R. is the court-appointed defense attorney for Story. Story is detained, has pleaded guilty pursuant to a plea agreement, and is pending sentencing.

11. I have been provided a July 18, 2021 email exchanged as part of discovery in Story's case. The email is also from brianbown@hotmail.com and was sent to Story's prior attorney (another federal defender at the FPD) at her work email address. The email is signed "Brian Bown," includes this email address in the signature line, and refers to knowing Story and offering to speak with the FPD.

12. Using law enforcement databases, I determined that Brian Bown resided at a mobile home park on Cave Creek Road. This is the same address at which Story was previously arrested by law enforcement in relation to his criminal case, where he was living with Bown. In the July 18 email referenced above, Bown also noted this, telling the then-assigned FPD attorney "I assume you know the Marshalls came to my house and grabbed Jerry." I conducted a drive-by of the address on October 22, 2021, and spoke with management at the mobile home park. The management confirmed to me that Bown resided at that address. I took photographs of the residence.

13. USMS offered to coordinate a request to local police to increase patrols in the area where the victim lives as a result of these threats. The victim requested that this occur. Thus, USMS has worked with local police to increase patrols in that area.

14. On October 23, 2021, Magistrate Judge John Z. Boyle authorized a criminal Complaint charging Bown with one count of Interstate Communications Involving a Threat, in violation of 18 U.S.C. § 875(c), and one count of Cyberstalking, in violation of 18 U.S.C. § 2261A(2) and 2261(b). *See United States v. Brian Gillespie Bown*, No. MJ 21-8259 (D. Ariz.). Judge Boyle also authorized an arrest warrant and a warrant to search Bown's residence and seize evidence related to this matter. *See* Case No. MB 21-8258 (D. Ariz.).

15. Later on October 23, 2021, USMS personnel executed the warrants at Bown's residence. Bown was taken into custody and is currently detained. Bown was advised of his *Miranda* rights and invoked his right to remain silent.

16. Based on my training and experience, I understand that Microsoft Corporation, headquartered in Redmond, Washington, is the service provider associated

with the Hotmail account used by Bown. This email service utilizes the internet, an international network of interconnected servers and computers throughout the country and the world, to provide the email services, which is an instrumentality of interstate and foreign commerce.

17. Based on information provided to me by other law enforcement personnel, I know that Bown has communicated about Story's criminal case with Story by telephone, as I have been informed that CoreCivic, where Story has been detained for portions of the pretrial proceedings in his criminal case, has jail calls in which Story and Bown discuss his case and Bown makes critical statements about Story's prior lawyer (then also an Assistant Federal Public Defender in the District of Arizona).

18. Evidence of Bown's commission of the target offenses, as well as evidence related to his intent, bias, and motivation for committing the target offenses, and his identity as the user of the device(s) that accessed the Hotmail account when the threatening messages were sent, is likely to be found in the contents of the Hotmail account listed in Attachment A. Because the relationship between Bown and Story, including the course of Bown's contact with Story during period of his pretrial confinement, appears to have been an element leading up to the threats being issued against Story's attorney, there is probable cause to believe that evidence regarding the subject offenses will be found in the email account to be searched going back at least to March 2, 2021 (the date of Story's initial arrest in his case).

19. In general, an email that is sent to a Microsoft subscriber is stored in the subscriber's "mail box" on Microsoft servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Microsoft servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Microsoft's servers for a certain period of time.

BACKGROUND CONCERNING EMAIL

20. In my training and experience, I have learned that Microsoft provides a variety of on-line services, including electronic mail ("email") access, to the public.

Microsoft allows subscribers to obtain email accounts at the domain name Hotmail.com, like the email account listed in Attachment A. Subscribers obtain an account by registering with Microsoft. During the registration process, Microsoft asks subscribers to provide basic personal information. Therefore, the computers of Microsoft are likely to contain stored electronic communications (including retrieved and unretrieved email for Microsoft subscribers) and information concerning subscribers and their use of Microsoft services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

21. A Microsoft subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Microsoft. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

22. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

23. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This

information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

24. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

25. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as

described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

26. Based on the forgoing, I request that the Court issue the proposed search warrant.

27. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Microsoft. Because the warrant will be served on Microsoft, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

//

//

//

//

//

//

28. This affidavit is being sworn telephonically before a United States Magistrate Judge legally authorized to administer an oath for this purpose. I have reviewed the affidavit and attest that there is sufficient evidence to establish probable cause that the defendant committed the crimes alleged.

Pursuant to 28 U.S.C. § 1746(2), I declare that the foregoing is true and correct to the best of my knowledge and belief.

Respectfully submitted,

Charles Rowland

Charles Rowland, Senior Inspector, USMS

Sworn to and subscribed telephonically on October 25, 2021. @ 11:36 a.m.

Deborah M. Fine

HONORABLE DEBORAH M. FINE
United States Magistrate Judge